UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P O Box 1450
Alexandria, Virginia 22313-1450
www uspto gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/565,663	01/23/2006	Franciscus L. A. J. Kamperman	NL 030926	2420

24737 7590 04/28/2011
PHILIPS INTELLECTUAL PROPERTY & STANDARDS
P.O. BOX 3001
BRIARCLIFF MANOR, NY 10510

EXAMINER	
KEEHN, RICHARD G	
ART UNIT	PAPER NUMBER
2456	

NOTIFICATION DATE	DELIVERY MODE
04/28/2011	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

vera.kublanov@philips.com
debbie.henn@philips.com
marianne.fox@philips.com

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Application Number: 10/565,663
Filing Date: January 23, 2006
Appellant(s): KAMPERMAN ET AL.

Michael A. Scaturro (51,356)
For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed 2/15/2011 appealing from the Office action mailed 8/27/2010.

(1) Real Party in Interest

The examiner has no comment on the statement, or lack of statement, identifying by name the real party in interest in the brief.

(2) Related Appeals and Interferences

The examiner is not aware of any related appeals, interferences, or judicial proceedings which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

(3) Status of Claims

The following is a list of claims that are rejected and pending in the application:

Claims 1, 3, 4, 6-12, 14, 15 and 17-23.

(4) Status of Amendments After Final

The examiner has no comment on the appellant's statement of the status of amendments after final rejection contained in the brief.

(5) Summary of Claimed Subject Matter

The examiner has no comment on the summary of claimed subject matter contained in the brief.

(6) Grounds of Rejection to be Reviewed on Appeal

The examiner has no comment on the appellant's statement of the grounds of rejection to be reviewed on appeal. Every ground of rejection set forth in the Office action from which the appeal is taken (as modified by any advisory actions) is being maintained by the examiner except for the grounds of rejection (if any) listed under the subheading "WITHDRAWN REJECTIONS." New grounds of rejection (if any) are provided under the subheading "NEW GROUNDS OF REJECTION."

NEW GROUND(S) OF REJECTION

None.

WITHDRAWN REJECTIONS

The following grounds of rejection are not presented for review on appeal because they have been withdrawn by the examiner. The rejection of Claim 23 under 35 U.S.C. 101, based on Appellant's after-final amendment submitted 10/27/2011.

(7) Claims Appendix

The examiner has no comment on the copy of the appealed claims contained in the Appendix to the appellant's brief.

(8) Evidence Relied Upon

2003/0018491 A1	Nakahara et al.	1-2003
6,324,645 B1	Andrews et al.	11-2001

(9) Grounds of Rejection

The following ground(s) of rejection are applicable to the appealed claims:

1. **Claims 1, 3, 4, 6-12, 14, 15 and 17-23 are rejected under 35 U.S.C. 103(a) as being unpatentable over US 2003/0018491 A1 (Nakahara et al.), and further in view of US 6,324,645 B1 (Andrews et al.).**

As to Claims 1, 12 and 23, Nakahara et al. disclose a method, a system for generating an Authorized Domain (AD), and computer readable medium having stored thereon instructions for causing one or more processing units to execute the method, of generating an Authorized Domain (AD), comprises:

selecting a domain identifier (Domain_ID) uniquely identifying the Authorized Domain (AD) (Nakahara et al. disclose the domain list – Pages 12-13, ¶ [0200]),

binding at least one user (P1, P2, ..., PN1) to the domain identifier (Domain_ID) (Nakahara et al. disclose searcher X belonging to the domain – Page 13, ¶¶ [0197 and 0200]),

binding at least one device (D1, D2, ..., DM) to the domain identifier (Domain_ID) (Nakahara et al. disclose the function units belonging to the domain – Page 13, ¶ [0200]), and

binding at least one content item (C1, C2, ..., CN2) to the Authorized Domain (AD) given by the domain identifier (Domain ID) (Nakahara et al. disclose the content usage devices belonging to the domain – Page 13, ¶ [0200]),

thereby obtaining a number of devices (D1, D2, ..., DM) and a number of users (P1, P2, ..., PN1) that are authorized to access content items (C1, C2, ..., CN2) of said Authorized Domain (AD) (Nakahara et al. disclose the domain list {Domain ID}, at least one user {user}, function units {devices}, and content usage devices {content items}, and licensing {authorized} – Pages 12-13, ¶ [0200])

wherein access to the at least one content item (C1, C2, ..., CN2) is obtained, via an authorized certificate, by verifying that the at least one content item (C1, C2, ..., CN2) and the at least one user (P1, P2, ..., PN1) are linked to the same domain identifier (Domain_ID) or by verifying that the at least one device (D1, D2, ..., DM) and the at least one content item (C1, C2, ..., CN2)) are linked to the same domain identifier (Domain_ID) (Nakahara et al. disclose granting or restricting access to content based on whether the user and content domain licensing requirements are met – Page 12, ¶ [0197]; via an authorized certificate - ¶ [0198]); and

wherein the authorized certificate (Nakahara et al. disclose authorized certificates - ¶ [0198]).

Nakahara et al. does not explicitly disclose including the domain identifier as a holder of the authorized certificate. However Andrews et al. disclose

includes the domain identifier (Domain_ID) as a holder of the authorized certificate (Andrews et al. disclose inclusion of the domain id as a holder of the authorized certificate – Column 9, lines 49-58).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine including the domain identifier as a holder of the authorized certificate taught by Andrews et al., with the use of authorized certificates taught by Nakahara et al., in order to to identify user priviliges (Andrews et al. - Column 9, lines 49-58).

As to Claims 3 and 14, the combination of Nakahara et al. and Andrews et al. discloses a method and system according to claims 1 and 12 respectively, wherein the binding at least one user (P1, P2, ..., PN1) to the domain identifier (Domain_ID) comprises:

obtaining or generating a Domain Users List (DUC) comprising the domain identifier (Domain_ID) and a unique identifier (Pers_ID1, Pers_ID2, ..., Pers_IDN1) for a user (P1, P2, ..., PN1) thereby defining that the user is bound to the Authorized Domain (AD) (Nakahara et al. disclose the domain list - ¶ [0200], which comprises the function unit ID and user ID fields - Figure 3),

and/or in that

the binding at least one device (D1, D2, ..., DM) to the domain identifier (Domain_ID) comprises:

obtaining or generating a Domain Devices List (DDC) comprising the domain identifier (Domain_ID) and a unique identifier (Dev.ID 1, Dev.ID2, ..., Dev.IDM) for a device (D1, D2, ..., DM) thereby defining that the device is bound to the Authorized Domain (AD) (Nakahara et al. disclose the domail list - ¶ [0200], which comprises the function unit ID and user ID fields - Figure 3).

As to Claims 4 and 15, the combination of Nakahara et al. and Andrews et al. discloses a method and system according to claims 1 and 12 respectively, wherein the binding at least one content item (C1, C2, ..., CN2) to the Authorized Domain (AD) comprises:

binding a content item (C1, C2, ..., CN2) to a User Right (URC1, URC2, ... URCN2), where said User Right (URC1, URC2, ... URCN2) is bound to a user (P1, P2, ..., PN1) bound to the Authorized Domain (AD), and/or

binding a content item (C1, C2, ..., CN2) to a Device Right (DevRC), where said Device Right (DevRC) is bound to a device (D1, D2, ..., DM) which is bound to the Authorized Domain (AD) (Nakahara et al. disclose the domain list {Domain ID}, at least one user {user}, function units {devices}, and content usage devices {content items}, and licensing {right to use} – Pages 12-13, ¶ [0200]), and/or

binding a content item (C1, C2, ..., CN2) to a Domain Rights (DRC1, DRC2, ... DRCN2), where said Domain Rights (DRC1, DRC2, ... DRCN2) is bound to the Authorized Domain (AD) (Nakahara et al. disclose the domain, content usage devices {content items}, and licensing {right to use} – Pages 12-13, ¶ [0200]).

As to Claims 6 and 17, the combination of Nakahara et al. and Andrews et al. discloses a method and system according to claims 4 and 15 respectively,

wherein the User Right (URC1, URC2, ..., URCN2) or the Device Right (DevRC) or the Domain Rights (DRC1, DRC2, ..., DRCN2) comprises rights data (Rghts Dat) representing which rights exists in relation to the at least one content item (C1, C2, ..., CN2) bound to the User Right (URC1, URC2, ..., URCN2) or the Device Right (DevRC) or the Domain Rights (DRC1, DRC2, ..., DRCN2) (Nakahara et al. disclose the domain list {Domain ID}, at least one user {user}, function units {devices}, and content usage devices {content items}, and licenses tied to the user, domain, devices and contents {right to use} – Pages 12-13, ¶ [0200]).

As to Claim 7 and 18, the combination of Nakahara et al. and Andrews et al. discloses a method and system according to claims 1 and 12 respectively, the method further comprises controlling access to a given content item bound to the Authorized Domain (AD) by a given device being operated by a given user, comprising:

checking if the given user is bound to the same Authorized Domain (AD) as the given content item, or

checking if the given device is bound to the same Authorized Domain (AD) as the given content item (Nakahara et al. disclose granting or restricting access to content based on whether the user and content domain licensing requirements are met – Page 12, ¶ [0197]),

and allowing access for the given user via the given device and/or other devices to the content item if the given user is bound to the same Authorized Domain (AD),

or allowing access for the given user and/or other users via the given device to the content item if the given device is part of the same Authorized Domain (AD) (Nakahara et al. disclose granting or restricting access to content based on whether the user and content domain licensing requirements are met – Page 12, ¶ [0197]).

As to Claims 8 and 19, the combination of Nakahara et al. and Andrews et al. discloses a method and system according to claims 3 and 14 respectively, the method further comprises controlling access to a given content item (C1, C2, ..., CN2), being bound to the Authorized Domain (AD) and having a unique content identifier (Cont ID), by a given device being operated by a given user comprising:

checking if the Domain Devices List (DDC) of the Authorized Domain (AD) comprises an identifier (Dev.ID) of the given device, thereby checking if the given device is bound to the same Authorized Domain (AD) as the content item, and/or checking if the Domain User List (DUC) of the Authorized Domain (AD) comprises an identifier (Pers_ID) of the given user (P1, P2, ..., PN1) thereby checking if the given user is bound to the same Authorized Domain (AD) as the content item (Nakahara et al. disclose granting or restricting access to content based on whether the user and content domain licensing requirements are met – Page 12, ¶ [0197]),

and allowing access to the given content item (C1, C2, ..., CN2) by the given device (D1, D2, ..., DM) for any user if the given device is bound to the same Authorized Domain (AD) as the content item being accessed, and/or

allowing access to the given content item (C1, C2, ..., CN2) by any device including the given device for the given user if the given user is bound to the same Authorized Domain (AD) as the content item being accessed (Nakahara et al. disclose granting or restricting access to content based on whether the user and content domain licensing requirements are met – Page 12, ¶ [0197]).

As to Claims 9 and 20, the combination of Nakahara et al. and Andrews et al. discloses a method and system according to claim 7 and 18 respectively,

wherein the binding at least one content item (C1, C2, …, CN2) to the Authorized Domain (AD) comprises:

binding a content item (C1, C2, …, CN2) to a User Right (URC1, URC2, …, URCN2) where said User Right (URC1, URC2, …, URCN2) is bound to a user (P1, P2, …, PN1) which is bound to the Authorized Domain (AD) (Nakahara et al. disclose the domain, content usage devices {content items}, and licensing {right to use} – Pages 12-13, ¶¶ [0197 and 0200]), and

wherein the controlling access of a given content item further comprises:

checking that the User Right (URC1, URC2, ..., URCN2) for a given content item specifies that the given user (P1, P2, ..., PN1) has a right to access the given content item (C1, C2, ..., CN2) and only allowing access to the given content item (C 1, C2, ..., CN2) in the affirmative (Nakahara et al. disclose granting or restricting access to content based on whether the user and content domain licensing requirements are met – Page 12, ¶ [0197]).

As to Claims 10 and 21, the combination of Nakahara et al. and Andrews et al. discloses a method according to claims 1 and 12 respectively,

wherein every content item is encrypted and that a content right (CR) is bound to each content item and to a User Right (URC) or a Device Right (DevRC) or a Domain Rights (DRC), and that the content right (CR) of a given content item comprises a decryption key for decrypting the given content item (Nakahara et al. disclose content encryption and decryption key - Page 3, ¶¶ [0048-0050]).

As to Claims 11 and 22, the combination of Nakahara et al. and Andrews et al. discloses a method and system according to claims 4 and 15 respectively, wherein

the Domain Users List (DUC) is implemented as or included in a Domain Users Certificate, and/or the Domain Devices List (DDC) is implemented as or included in a Domain Devices Certificate, and/or

the User Right (URC 1, URC2, ..., URCN2) is implemented as or included in a User Right Certificate, and/or

the Device Right (DevRC) is implemented as or included in a Device Right Certificate, and/or

the Domain Rights (DRC 1, DRC2, ..., DRCN2) is implemented as or included in a Domain Rights Certificate (Nakahara et al. disclose license authentication included in a certificate - ¶¶ [0198] [0249-0251] [0258]).

(10) Response to Argument

1. Appellant argues that Nakahara does not teach or suggest at least the step of "binding at least one user (P1, P2, ..., PN1) to the domain identifier (Domain_ID)." (Brief at 14). Appellant argues that "Searcher X cited in the reference is a pseudonym for a kind of role that a device/unit may have, but not a user." (Brief at 15). First of all, the claim requires "binding at least one *user*." The term "*user*" is not defined as a "person" or "human" in Claims 1 and 12. Therefore, using the broadest reasonable interpretation, a user may be a device. Furthermore, there is nothing in Claims 1 and 12 that make devices and users mutually exclusive. Nonetheless, it is clear from ¶ [0197] of Nakahara et al., which was cited in the Final Office action, that person-binding is taught by the reference. Paragraph [0197] recites:

> "For example, even if ***someone*** connects an unauthorized terminal device located outside of the home network 300 to the home network 300 to acquire

> license information, ***he*** cannot acquire the license information because the terminal device ***does not belong to the identical user domain***. ***Also***, if different usage restrictions are put on a content usage device 1 for a ***father's usage*** and a content usage device 2 for his ***son's usage*** within the home network 300, these content usage devices can be classified so that the ***son*** cannot acquire the license information on the content usage device 2 though his ***father*** can acquire it on the content usage device 1." {***emphasis*** by Examiner}

From the foregoing, it is clear that persons are bound to the domain, because a father's {a person's} rights are bound, a son's {another person's} rights are bound, and the restriction applied is based on the person bound to the domain (father or son). Furthermore, ¶ [0198] clearly indicates authenticating the *user* domain. Taking this in context with ¶¶ [0014-0016 and 0197], where "a *user* can operate the content usage device", it is clear that users can be people in Nakahara et al. Appellant also argues that Nakahara does not disclose users as identifiers included in data structures, represented as elements of the domain structure." (Brief at 14). But this is not claimed. Appellant's claims recite binding at least one user, not that a user is an identifier, nor that a user is an element of the domain structure. The users are merely *bound* to the domain as claimed. This claim language does not not necessarily make the users "elements of the domain" as argued by Appellant. Therefore, Appellant argues that which has not been claimed. Nonetheless, Nakahara's father and son are certainly bound to the domain since their individual rights are being authenticated; which also makes the father and son identifiers in the domain.

2. Appellant argues that Nakahara does not teach or suggest the limitations: "binding at least one content item (C1, C2, ..., CN2) to the Authorized Domain (AD) given by the domain identifier (Domain_ID)"; and "thereby obtaining a number of devices (D1, D2, ..., DM) and a number of users (P1, P2, ..., PN1) that are authorized to access content items (C1, C2, ..., CN2) of said Authorized Domain (AD)." (Brief at 15). To support this assertion, Appellant argues that "'content usage devices' are entirely different from 'content items'", but fails to argue or support how the broad claim term "item" has to be narrowly construed to *exclude* a device. (Brief at 15) An "item" can certainly be a "device." In addition, it is clear from ¶ [0197] discussed above, and ¶¶ [0193-0194] that licenses are also bound to the domain, and licenses are intangibles, not devices. License data are also content items. Therefore it is clear that Nakahara et al. disclose content items bound to the domain.

3. Appellant argues that Nakahara does not teach or suggest "via an authorization certificate." (Brief at 16). To support this assertion, Appellant says that "Nakahara clearly states that the certificate is purely a regular identity certificate used to identify a component, which is different from a domain related certificate." (Brief at 16). First, the claim requires "via an authorization certificate", not "via a domain related certificate." The certificate in ¶ [0198] of Nakahara is an authorization certificate. Second, Nakahara's authorized certificate is also domain-related based on the phrase "before it authenticates using the user domain and usage restriction." Clearly, the certificate is related to authenticating access to domain resources> Therefore the certificate is domain-related.

4. Appellant argues that the cited references fail to disclose "inclusion of the domain id as a holder of the authorized certificate" by arguing that "[A]ccording to the invention, a certificate creates or defines part of the domain." (Brief at 16) Examiner has to examine what is claimed. The claim does not recite that “a certificate creates or defines part of the domain”, as argued by Appellant. Instead, the claim limitation recites “wherein the authorization certificate includes the domain identifier (Domain_ID) as a holder of the authorization certificate.” Examiner relied upon Andrews et al. to teach “includes the domain identifier (Domain_ID) as a holder of the authorized certificate.” Clearly, Andrews discloses this limitation at 9:49-58. This cited section teaches that the digital certificates contain an access label {holder} that is used to identify which user(s) have privileged access to content within a domain {holder of the certificate}; and that access label includes a domain identifier. Even according to Appellant's argued definition of "a certificate creates or defines part of the domain", the domain identifier in the Andrews identifies which domain the certificate applies to, which is “part of the domain”. Nonetheless, there is absolutely nothing in the language of the argued Claims 1 and 12 that indicates that “a certificate creates or defines part of the domain." Appellant’s argument that the claimed invention relates to content-access domains vs. Andrews relating to privilege/administrative domains is unpersuasive to the Examiner because both inventions are related to privileged access to content within a domain.

5. The remainder of Appellant’s brief (bottom of Page 16 through page 22) does not contain argument, but rather further defines the invention by way of examples and definitions.

6. Examiner rejected Claim 23, and dependant claims 3, 4, 6-11, 14, 15 and 17-22, under 35 U.S.C. 103(a). Appellant has not argued against this rejection. Therefore, the rejection is respectfully maintained.

7. Examiner rejected Claim 23 based on 35 U.S.C. 101. Appellant has not argued against this rejection, but has amended the claim to overcome the rejection. Therefore, the rejection of Claim 23 under 35 U.S.C. 101 has been respectfully withdrawn.

(11) Related Proceeding(s) Appendix

No decision rendered by a court or the Board is identified by the examiner in the Related Appeals and Interferences section of this examiner's answer.

For the above reasons, it is believed that the rejections should be sustained.

Respectfully submitted,

/RICHARD G KEEHN/

Examiner, Art Unit 2456

Conferees:

/YASIN BARQADLE/
Primary Examiner, Art Unit 2456

/Rupal D. Dharia/
Supervisory Patent Examiner, Art Unit 2456